UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/699,947	11/03/2003	Sajosh Janarthanam	PJW181	4353

7590 07/13/2007

Paul J. Winters
307 Cypress Point Drive
Mountain View, CA 94043

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	**PAPER NUMBER**
2132	
MAIL DATE	**DELIVERY MODE**
07/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/699,947	**Applicant(s)** JANARTHANAM ET AL.
	Examiner Samson B. Lemma	**Art Unit** 2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 April 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3 and 5-10* is/are rejected.

7)☒ Claim(s) *4,11 and 12* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on April 17, 2007. No claim is canceled/added. Claims 1-12 **are pending/examined.**

2. Applicant amended claim 8 and overcome the objection set forth in the pervious office action. Therefore the objection made to claim 8 is withdrawn.

Priority

3. This application does not claim priority of an application. Therefore, the effective filling data for the subject matter defined in the pending claims of this application is **11/03/2003.**

Response to Arguments

4. Applicant's remark/arguments filed on April 17, 2007 have been fully considered but they are not persuasive.

Applicant argument is based on the reference used in rejecting the corresponding limitation recited in the claims 1-3 and 5-10. Applicant in particular argued that the following limitations which is recited in claims 1 and 6-7, **"comparing a characteristic of the encrypted data string with a characteristic of the second data string"** is neither disclosed by the admission prior art nor by the secondary reference on the record namely **Ferrant**.

Applicant wrote the following in support of his argument.

"In Ferrant, the procedure is that all the data stored in a memory is received, and is acted on according to an encryption algorithm. This apparently corresponds to the first data string of claim 1, which is encrypted using an encryption algorithm. In Ferrant, this encrypted data string is compared with "the result expected from the memory data". In applicants' claim 1, the comparison is between the encrypted

data string and the second data string which is in a memory structure. There is no disclosure in Ferrant that the "second data string" is in a memory structure as called for in claim 1. Rather, Ferrant only talks of an expected result based on memory data. It is therefore respectfully submitted that even if the Admission were combined with the disclosure of Ferrant, the resulting method would not anticipate applicants' claim 1."

Examiner disagrees with the above argument.

Examiner would point out that on the abstract, the following has been disclosed by *Ferrant* /secondary reference on the record that shows/confirms that the expected value/second data string is stored in the memory structure before it is compared with the calculated value/first string.

"A ROM including an array, each cell of which is accessible by means of a column address and of a row address, includes a **parity memory for storing the expected parity** of each row and of each column, an electrically programmable one-time programmable address memory, a testing circuit for, during a test phase, calculating the parity of each row and of each column, **comparing the calculated and expected parities** for each row and each column" [See abstract]

Furthermore Examiner would point out that on column 1, lines 23-27 the following has been disclosed which is equivalent to what is already disclosed above on the abstract which also meets the limitation recited as ***comparing a characteristic of the encrypted data string with a characteristic of the second data string.***

"Such a device is designed for, during a test phase, successively receiving all the data stored in the memory, adding them, multiplying them, etc. according to an adequate encryption algorithm, and comparing the final result **with the result**

expected from the memory data. When the results are equal, the memory is assumed to be good." [See column 1, lines 23-27]

Indepenent claims 6 and 7 recites similar limitation as that of independent claim 1, therefore examiner response shown above is also applicable to these independent claims.

In order to show how each and every limitation of the independent claims is disclosed by the reference on the record namely by the combination of admission prior art and *Ferrant Examiner would show the following.*

As per independent claims 1, Admission discloses a method of testing a device *[Title "testing the encryption function device" or see also on page 1, "DUT"/ device under the test")* **comprising:**

- **Providing a first data string** *[Page 2, lines 14-18, "P1S1", see also figure 1, ref. Num "P1S1"];*
- **Providing a second data string in a memory structure [page 2, lines 26-36 and figure 3, ref. Num "eP1S2"];**
- **Encrypting the first data string** *[See figure 1, ref. "P1S1"]* **using an encryption algorithm** *[see page 2, lines 14-18, "AES"],* **to provide an encrypted data string;** *[Page 2, lines 14-18, "eP1S1", see also figure 1, ref. Num "eP1S1"];*

and

- **Comparing a characteristic of the encrypted data string with a characteristic of the second data string.[page 6, lines 14-19]** *(" While it would be of course desirable to test the encryption function of the DUT for proper operation thereof, i. e., that the encrypted packet data string is as expected, the* ***matching of resulting encrypted packet data segment against each of the possible encrypted forms is impractical,*** *because of the very large number of* *possible encrypted forms. Therefore, what is needed is a method for testing the encryption function of a device, which method is simple and effective in use.")*

- Admission does not explicitly disclose,

Comparing a characteristic of the encrypted data string with a characteristic of the second data string.

However, in the field of endeavor **Ferrant**, discloses way of testing the proper manufacturing of a ROM consists of reading its content and checking that all the stored information is correct. This test operation is lengthy and expensive, and an embarked testing device is included in a ROM. Such a device is designed for, during a test phase, successively receiving all the data stored in the memory, **adding them, multiplying them, etc. according to an adequate encryption algorithm, and comparing the final result with the result expected from the memory data.** When the results are equal, the memory is assumed to be good, which meets the limitation of "comparing **a characteristic of the encrypted data string with a characteristic of the second data string."** *[Column 1, lines 8-33] and Furthermore Ferrant* /secondary reference on the record that shows/confirms that the expected value/second data string is stored in the memory structure before it is compared with the calculated value/first string. "A ROM including an array, each cell of which is accessible by means of a column address and of a row address, includes a **parity memory for storing the expected parity** of each row and of each column, an electrically programmable one-time programmable address memory, a testing circuit for, during a test phase, calculating the parity of each row and of each column, **comparing the calculated and expected parities** for each row and each column" [See abstract]

<u>As per independent claims 6-7, Admission discloses a</u> method of testing a device *[Title "testing the encryption function device" or see also on page 1, "DUT"/ device under the test")* **comprising:**

- **Providing a first data string** *[Page 2, lines 14-18, "P1S1", see also figure 1, ref. Num "P1S1"];*
- **Providing a second data string in a memory structure [page 2, lines 26-36 and figure 3, ref. Num "eP1S2"];**
- **Encrypting the first data string** *[See figure 1, ref. "P1S1"]* **using an encryption algorithm** *[see page 2, lines 14-18, "AES"],* with an initialization vector applied in such encryption,*[Page 2, lines 14-18, see initialization vector "IVAES1", see also figure 1, ref. "IVAES1")* **to generate an encrypted data string;** *[Page 2, lines 14-18, "eP1S1", see also figure 1, ref. Num "eP1S1"];*

and

- **Comparing an initialization vector associated with the encrypted data string with an initialization vector applied in encrypting the first data string.[page 6, lines 14-19]** *(" While it would be of course desirable to test the encryption function of the DUT for proper operation thereof, i. e., that the encrypted packet data string is as expected, the* ***matching of resulting encrypted packet data segment against each of the possible encrypted forms is impractical,*** *because of the very large number of possible encrypted forms. Therefore, what is needed is a method for testing the encryption function of a device, which method is simple and effective in use.")*
- Admission does not expressly disclose,

Comparing a characteristic of the encrypted data string with a characteristic of the second data string.

However, in the field of endeavor **Ferrant**, discloses way of testing the proper manufacturing of a ROM consists of reading its content and checking that all the stored information is correct. This test operation is lengthy and expensive, and an embarked testing device is included in a ROM. Such a device is designed for, during a test phase, successively receiving all the data stored in the memory, **adding them, multiplying them, etc. according to an adequate encryption algorithm, and comparing the final result with the result expected from the memory data.** When the results are equal, the memory is assumed to be good, which meets the limitation of "comparing **a characteristic of the encrypted data string with a characteristic of the second data string."** *[Column 1, lines 8-33]. Furthermore Ferrant* /secondary reference on the record that shows/confirms that the expected value/second data string is stored in the memory structure before it is compared with the calculated value/first string. "A ROM including an array, each cell of which is accessible by means of a column address and of a row address, includes a **parity memory for <u>storing the expected</u> parity** of each row and of each column, an electrically programmable one-time programmable address memory, a testing circuit for, during a test phase, calculating the parity of each row and of each column, **comparing the calculated and <u>expected</u> parities** for each row and each column" [See abstract]

In response to applicant's arguments against the references individually, especially focusing on the secondary reference namely Ferrant, Examiner would like to point out that one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references (Here the rejection is the combination of Ferrant and admitted prior art). See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

The other argument presented by the applicant is related to the dependent claims.

Examiner disagrees with the argument as the dependent claims stands and falls with the corresponding independent claims.

Therefore all limitations recited in the independent claims are undoubtedly disclosed by the reference/s on the record and the rejection is maintained until the applicant amends the independent claims and successfully overcome the rejection without introducing new matters.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 1-3 and 5-10** are rejected under 35 U.S.C. 103(a) as being unpatentable over admitted prior art (hereinafter referred to as **Admission**) (Provided Specification) in view of **Richard Ferrant** (hereinafter referred as **Ferrant**) (U.S. Patent No 6,421,799 B1) (Date of Patent: July 16, 2002)

7. **As per independent claims 1, Admission discloses a method of testing a device** *[Title "testing the encryption function device" or see also on page 1, "DUT"/device under the test")* **comprising:**

- **Providing a first data string** *[Page 2, lines 14-18, "P1S1", see also figure 1, ref. Num "P1S1"];*
- **Providing a second data string in a memory structure [page 2, lines 26-36 and figure 3, ref. Num "eP1S2"];**

- **Encrypting the first data string** *[See figure 1, ref. "P1S1"]* **using an encryption algorithm** *[see page 2, lines 14-18, "AES"],* **to provide an encrypted data string;** *[Page 2, lines 14-18, "eP1S1", see also figure 1, ref. Num "eP1S1"];*

and

- **Comparing a characteristic of the encrypted data string with a characteristic of the second data string.[page 6, lines 14-19]** *(" While it would be of course desirable to test the encryption function of the DUT for proper operation thereof, i. e., that the encrypted packet data string is as expected, the* ***matching of resulting encrypted packet data segment against each of the possible encrypted forms is impractical,*** *because of the very large number of possible encrypted forms. Therefore, what is needed is a method for testing the encryption function of a device, which method is simple and effective in use.")*
- Admission does not explicitly disclose,

Comparing a characteristic of the encrypted data string with a characteristic of the second data string.

However, in the field of endeavor **Ferrant**, discloses way of testing the proper manufacturing of a ROM consists of reading its content and checking that all the stored information is correct. This test operation is lengthy and expensive, and an embarked testing device is included in a ROM. Such a device is designed for, during a test phase, successively receiving all the data stored in the memory, **adding them, multiplying them, etc. according to an adequate encryption algorithm, and comparing the final result with the result expected from the memory data.** When the results are equal, the memory is assumed to be good, which meets the limitation of "comparing **a characteristic of the encrypted data string with a characteristic of the second data string."** *[Column 1, lines 8-33] Furthermore Ferrant /* secondary reference on the record that shows/confirms that the expected value/second data string is stored in the memory structure before it is compared with the calculated value/first string. "A ROM including an array, each cell of which is accessible by means of a column address and of a row address, includes a **parity memory for <u>storing the expected</u> parity** of each row and of each column, an electrically programmable one-time programmable address memory, a testing circuit for, during a test phase, calculating the parity of each row and of each column, **comparing the calculated and <u>expected</u> parities** for each row and each column" [See abstract]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature of comparison as per teachings of **Ferrant**, in to the method as taught by Admission, in order to provide effective testing mechanism. [See column 1, lines 18-35]

8. **<u>As per independent claims 6-7, Admission discloses a</u> method of testing a device** *[Title "testing the encryption function device" or see also on page 1, "DUT"/ device under the test")* **comprising:**

- **Providing a first data string** *[Page 2, lines 14-18, "P1S1", see also figure 1, ref. Num "P1S1"];*
- **Providing a second data string in a memory structure [page 2, lines 26-36 and figure 3, ref. Num "eP1S2"];**
- **Encrypting the first data string** *[See figure 1, ref. "P1S1"]* **using an encryption algorithm** *[see page 2, lines 14-18, "AES"]*, with an initialization vector applied in such encryption,*[Page 2, lines 14-18, see initialization vector "IVAES1", see also figure 1, ref. "IVAES1")* **to generate an encrypted data string;** *[Page 2, lines 14-18, "eP1S1", see also figure 1, ref. Num "eP1S1"];*

and

- **Comparing an initialization vector associated with the encrypted data string with an initialization vector applied in encrypting the first data string.[page 6, lines 14-19]** *(" While it would be of course desirable to test the encryption function of the DUT for proper operation thereof, i. e., that the encrypted packet data string is as expected, the* ***matching of resulting encrypted packet data segment against each of the possible encrypted forms is impractical,*** *because of the very large number of possible encrypted forms. Therefore, what is needed is a method for testing the encryption function of a device, which method is simple and effective in use.")*
- Admission does not expressly disclose,

Comparing a characteristic of the encrypted data string with a characteristic of the second data string.

However, in the field of endeavor **Ferrant**, discloses way of testing the proper manufacturing of a ROM consists of reading its content and checking that all the stored information is correct. This test operation is lengthy and expensive, and an embarked testing device is included in a ROM. Such a device is designed for, during a test phase, successively receiving all the data stored in the memory, **adding them, multiplying them, etc. according to an adequate encryption algorithm, and comparing the final result with the result expected from the memory data.** When the results are equal, the memory is assumed to be good, which meets the limitation of "comparing **a characteristic of the encrypted data string with a characteristic of the second data string."** *[Column 1, lines 8-33] Furthermore Ferrant* /secondary reference on the record that shows/confirms that the expected value/second data string is stored in the memory structure before it is compared with the calculated value/first string. "A ROM including an array, each cell of which is accessible by means of a column address and of a row address, includes a **parity memory for <u>storing</u>**

the expected parity of each row and of each column, an electrically programmable one-time programmable address memory, a testing circuit for, during a test phase, calculating the parity of each row and of each column, **comparing the calculated and expected parities** for each row and each column" [See abstract]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature of comparison as per teachings of **Ferrant**, in to the method as taught by Admission, in order to provide effective testing mechanism. [See column 1, lines 18-35]

9. **As per dependent claims 2-3 and 8-10, the combination of Admission and Ferrant discloses a method as applied to claims above. Furthermore, Admission discloses the method wherein, the step of comparing a characteristic of the encrypted data string with a characteristic of the second data string comprises comparing the bit length of the encrypted data string with the bit length of the second data string**. **[page 1, line 16, page 6, lines 14-19]** *(" While it would be of course desirable to test the encryption function of the DUT for proper operation thereof, i. e., that the encrypted packet data string is as expected, the* ***matching of resulting encrypted packet data segment against each of the possible encrypted forms is impractical,*** *because of the very large number of possible encrypted forms. Therefore, what is needed is a method for testing the encryption function of a device, which method is simple and effective in use." And on page 1, lines 16 of the applicant's specification discloses that the properties of the data* ***packets includes packet length)***

10. **As per dependent claim 5, the combination of Admission and Ferrant discloses a method as applied to claims above. Furthermore, Admission discloses**

the method wherein, the data string in the memory structure is an unencrypted data string. *[See figure 1, ref, "P1S1" and figure 2, ref. "P1S2"]*

Allowable Subject Matter

11. **Claims 4 and 11-12** are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
SL
07/01/2007

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100